COMMONWEALTH OF VIRGINIA

Information Technology Resource Management Guideline:

NETWORKING AND TELECOMMUNICATIONS GUIDELINE

Department of Technology Planning

Preface

Publication Designation

COV ITRM Guideline NET2001-01.1

Subject

Networking and Telecommunications

Effective Date

December 7, 2001

Supersedes

COV ITRM Guideline 95-1, Local Area Networks, dated January 31, 1995

Scheduled DTP Review

One (1) year from effective date

Authority

Code of Virginia, § 2.2-226
(Powers and Duties of the Secretary)

Code of Virginia, § 2.2-2651
(Powers and Duties of the Council on Technology Services)

Code of Virginia, § 2.2-1701
(Powers and Duties of the Department of Technology Planning)

Code of Virginia, §2.2-1303
(Powers and Duties of the Department of Information Technology)

Scope

This guideline is applicable to all state agencies and institutions of higher education (hereinafter collectively referred to as "agencies") that are responsible for local and wide-area networking or telecommunications. Local government entities are encouraged to review this guidance as well.

Purpose

Sharing best practices in telecommunications and networking may aid state agencies in reducing cost, improving management practices, and improving communications between the government and its citizens.

Objectives

To provide agencies with guidance related to networking and telecommunications infrastructure development, maintenance and administration.

To provide agencies with guidance related to local and wide area network services.

General Responsibilities

In accordance with the *Code of Virginia*, the following provisions apply:

Secretary of Technology

Responsible for:

- Directing the formulation and promulgation of policies, standards, specifications, and guidelines for information technology in the Commonwealth, including, but not limited to, those (i) required to support state and local government exchange, acquisition, storage, use, sharing, and distribution of geographic or base map data and related technologies and (ii) concerning the development of electronic transactions including the use of electronic signatures as provided in § 59.1-496.

Council on Technology Services (COTS)

Responsible for :

- Advising and assisting the Secretary of Technology in exercising the powers and performing the duties conferred.

Department of Technology Planning (DTP)

Responsible for:

- Developing and promulgating policies, standards, and guidelines for managing information technology in the Commonwealth.

All State Agencies

Responsible for:

- Complying with the Department of Technology Planning's policies, standards, and guidelines for information technology resources in the Commonwealth.

Definitions

Networking means any local, wide-area, metropolitan-area or campus network established for use by agencies of the Commonwealth.

Telecommunications means any transmission, emission, or reception of signs, signals, writings, images, and sounds, or information of any nature by wire, radio, visual, optical, or other electromagnetic systems.

Related COV ITRM Policies, Standards, and Guidelines

COV ITRM Policy NET2001-01.1, Networking and Telecommunications

COV ITRM Standard NET2001-01.1, Networking, Telecommunications, and Cabling

Table of Contents

Background

Earlier Commonwealth telecommunications standards and guidelines focused on building wiring. The COV ITRM Guideline NET2001-1.1 provides best practices in all areas of networking and telecommunications. This guidance emanates from the work of the Enterprise Architecture Network Domain team. This team included state agency, local government, and higher education members.

Approach

This document will provide a listing of best practices for networking and telecommunications. Every effort will be made to ensure that this guidance information is reviewed annually for continued applicability.

Reviews

A full review of the COV ITRM Guideline NET2001-01.1 is anticipated annually.

Statement of ITRM Best Practices for Networking and Telecommunications

The following ITRM best practices address various aspects of providing and managing the infrastructure needed to ensure effective voice, data, and video telecommunications services in the Commonwealth. This infrastructure is a critical resource needed to conduct the business of the Commonwealth. Guidance is provided for both local area and wide area networking (LAN and WAN).

Best Practice 1.   *State and Local Agency Interconnections for Telecommunications.*
For state and local agencies that need to communicate with one another, use of COVANET is strongly recommended as a cost-effective vehicle (i.e., for new contracts). Agencies are responsible for providing the gateway between their network and COVANET. Institutions of higher education may have alternate school-to-school connections for distance education or research (e.g., Internet 2) that should be leveraged rather than using COVANET.

Best Practice 2.   *Network Planning and Application Changes*. State and local agencies should ensure that network planning is well integrated with applications design/acquisition and roll out. From the application analysis stage through the design/acquisition stage, agencies should review application bandwidth requirements, real-time data flow needs, and expected system capacity changes from other sources. These reviews should be conducted quarterly.

Best Practice 3.   *Strategic Planning.* State and local agency heads should review business changes with networking staff or network providers to ensure network implications are addressed in a timely manner. Changes in business volume, staffing

levels, applications, or facilities (e.g., relocation, construction, or renovations) may affect network services.

Best Practice 4.   *Telecommunications Service Change Planning.* State and local agency telecommunications planners should confer with the Department of Information Technology (DIT) regarding the amount of lead-time required to make service changes involving DIT telecommunications contracts. (DIT holds Telecommunications contracts for state agencies in the Commonwealth as provided in the *Code of Virginia,* § 2.1-563.17. Powers and duties.)

Best Practice 5.   *Domain Name Systems (DNS).* State and local agencies should have a primary and a secondary DNS server (required for domain registration), each of which should reside on a separate network. This practice enables the agency Web site to remain visible to users if one network is down. DIT provides a secondary DNS server for COVANET customers. [1]

Best Practice 6.   *Planning for Voice, Video and Data.* When designing new networks, state and local agencies should design for voice, video, data, and image traffic on the network. Although Gigabit Ethernet is rarely provided to the desktop, it is in common use as a backbone technology and should be considered. Examples of other design components to address potential future business needs are layer three intelligent switches, layer four bandwidth management facilities, and switched 100 Mbps Ethernet service. Few, if any, agency applications warrant Gigabit Ethernet to the desktop.

Best Practice 7.   *Network Planning and Risk.* State and local agencies should allow security and risk planning decisions to drive decisions regarding network design for redundancy, fail-over, and disaster recovery.

Best Practice 8.   *Wireless LANs.* State and local agencies should implement wireless LANs only when they have good business reasons to implement them and cost/benefit justifications. Agencies should consider the more frequent need for equipment changes for wireless infrastructure when assessing costs and benefits. For most implementations, the IEEE 802.11b standard should be implemented. All devices used for wireless LANs should carry the Wireless Ethernet Compatibility Alliance's (WECA) WiFi interoperability certification. For a current list see: http://www.wirelessethernet.org/.

Best Practice 9.   *Wireless Services*. State and local agencies deploying wireless LAN/WAN services should conduct thorough site survey including testing/inspection.

Best Practice 10.   *Test Environment.* When adding new applications to a network, state and local agencies should establish a test environment (platform). Agencies should use a parallel network infrastructure (in-house environment or vendor provided environment). The test environment should not exceed the requirements of the planned operational environment. An alternative to a test environment would be use of a controlled, measured implementation (validates network needs above).

---

[1] See Middleware Guidelines for additional discussion of DNS.

Whenever possible, the development environment should model and not exceed the infrastructure of the planned operational network environment (e.g., available bandwidth).

Best Practice 11.   *LAN Bandwidth Management*

- *(Switches).* Network administrators serving state and local agencies should convert central hubs to switches to realize an instant performance increase and to enable better management of bandwidth, even in a 10 Mbps Ethernet or a Token Ring environment. Switches operate at layer 2 in the manner of multiple bridges, vastly reducing collisions, and thus, the need for repeat traffic. The old hub can be connected to the switch to cascade bandwidth to low-end users.

- *(Bottlenecks).* Network administrators should identify the bottlenecks responsible for throughput degradation and attempt to address them. Workstations, RAIDs, and servers can be involved. Just upgrading from 10 Mbps to 100 Mbps Ethernet service may not fix a workstation or server I/O problem. If equipment is old, it may not have a PCI slot for a 10/100 NIC.

- *(Re-segmenting).* Network administrators should consider re-segmenting a LAN segment when sustained usage exceeds 50% on a regular basis.

- *(Routers).* Routers are slow and can be the cause of a bottleneck. Network administrators should replace internal routers with layer 3 switches to achieve a performance boost.

Best Practice 12.   *WAN Bandwidth Management.* Whenever WAN bandwidth usage is sustained at 50% or higher or future usage is forecast at 50% or higher, network administrators should determine the causes and attempt to alleviate the contention. If unable to reduce the contention through means such as rescheduling, the network administrator should consider increasing bandwidth.

Best Practice 13.   *New Technologies.* The Commonwealth should put into place a mechanism for monitoring new, key LAN and WAN services and technologies. As the services or technologies become more fully accepted, viable, available, and supportable, information regarding their availability should be conveyed to Agency Information Officers (AIOs) and other decision makers. The domain team should ensure the information is integrated into the *Networking Architecture*. DTP is the coordinating agency.

Best Practice 14.   *Single Pipeline.* If all federal security and cost issues could be resolved and if all state and local governments would use COVANET, single pipeline efficiencies in costs and management could be realized. The following current problems would be addressed.

- *Local service branches of state agencies often must support multiple connections to state and county/or city government offices.*

- *Local governments often must support connections to multiple state agencies and local agencies.*

- *State agencies must often support connections to multiple local agencies and to multiple state agencies.*

The COTS State and Local Network Integration Workgroup (SLANI) proposed a single pipeline solution. The network domain team recommends that COTS support this concept by forming a workgroup to develop a strategy for addressing each of the barriers to the single pipeline. The strategy might, for example, include working with the federal agencies to obtain traffic mingling agreements and cost allocation method agreements.

Best Practice 15. *Expertise Pooling.* COTS should develop a mechanism for informal sharing of expertise across agencies, including DIT. An example would be technology topic meetings, user groups, or sharing of briefing papers from investigating technologies.

Best Practice 16. *Remote Deployment*. In situations where technical staffs are not locally available, state and local agencies should consider the management, maintenance and service issues associated with remote deployments.

Best Practice 17. *Electrical Service*. State and local agency network infrastructure addition and/or revision plans should include an analysis of the adequacy of electrical service. Also, agencies should provide adequate electrical outlets for application testing infrastructure.

Best Practice 18. *UPS.* State and local agencies are strongly encouraged to use continuous inversion, uninterruptible power supply units (UPSs) with power conditioning. The UPS units should provide 15 minutes of battery backup for most network equipment and 30 minutes for servers. UPS units that automatically shut down in a controlled manner are preferred for servers.

Best Practice 19. *Telecommunicatoin Rooms (e.*g., Telecommunications Closets or Wiring Closets). State and local agencies should provide a secure, climate-controlled area for servers and networking components (e.g., switches, routers, etc.). Agencies are encouraged to use racks or cabinets to maximize the utility of space available and to ensuring adequate space for easy access to the front and rear of network equipment and servers. Telecommunications Rooms and space considerations are addressed in TIA/EIA-569.

Glossary

Agency Information Officer (AIO) - VA law requires certain state agencies to appoint an AIO.

Bandwidth - The carrying capacity of a circuit, usually measured in bits per second for digital circuits or hertz for analog circuits.

COVANET – COVANET is a comprehensive array of communications services, voice long distance, data, and Internet services to local and county governments, state agencies, universities, and quasi-government agencies.

Council on Technology Services (COTS) – COTS is an advisory group for Virginia's Secretary of Technology.

Ethernet – 1. A local-area network (LAN) protocol that is specified in IEEE 802.3 and that uses CSMA-CD to provide 10 Mbps service over copper; 2. any of various enhancements to Ethernet service providing greater bandwidth (e.g., Fast Ethernet or Gigabit Ethernet).

Fast EtherChannel – A Cisco proprietary method for increasing bandwidth by aggregating ports. The following link provides Fast EtherChannel literature:
http://www.cisco.com/warp/public/cc/techno/media/lan/ether/channel/prodlit/index.shtml

Hub - A LAN wiring concentrator that connects cables from numerous network devices. An intelligent hub can monitor and report on network activity, typically using SNMP.

Internet Protocol (IP) - A communications protocol, which is instrumental in routing packets of data from one node on the Internet to another. IPv4 routes each packet based on a 32 bit destination address called an IP address (e.g., 123.122.211.111).

IPv4 – Ipv4 is a four octet 32 bit IP address in the form 255.255.255.255.

IPv6 – Ipv6 is a sixteen octet 128 bit IP address. IPv6 identifies interfaces, not nodes. These addresses are of 3 types, unicast, multicast, and anycast. For a discussion and comparison with IPv4 see the following NCS literature:

http://www.ncs.gov/n6/content/tibs/html/tib97_1/sec5_0.htm.

Local Area Network (LAN) - A private computer network generally on a user's premises and operated within a limited geographical area.

Network - 1. A configuration of data processing devices and software connected for information interchange. 2. A group of two or more computer systems linked together.

Redundant Array of Independent Disks (RAID) - A method of organizing small format disk devices to drastically increase I/O bandwidth and improve data availability.

Router - 1. An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. 2. (IRM) The combination of hardware and software that links LANs and WANs together.

Segment -1. vt. to isolate traffic on a LAN; 2. n., the LAN devices and media isolated.

Simple Network Management Protocol (SNMP) - A set of network communication specifications that cover all the basics of network management. It is a simple and expandable protocol designed to give the capability to remotely manage a computer network by polling, setting terminal values, and monitoring network events. It is comprised of three elements, an MIB, a manager, and the agents. The manager is located on the host computer on the network. Its role is to poll the agents and request information concerning the networks status. Agents run off each network node and collect network and terminal information as specified in the MIB.

SLANI - State and Local Government Network Integration subcommittee of COTS (1998-2000)

Switch - 1. n., a circuit switching hub. 2. vt., A communications paradigm in which a dedicated communication path is established between the sender and receiver along which all packets travel. The telephone system is an example of a circuit switched network.

Wide Area Network (WAN) - 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. 3. A computer network that links multiple workstations and other devices across a large geographical area. A WAN typically consists of multiple LANs that are linked together.

Information provided in this Glossary was developed using several excellent Internet sources including the following:

O'Reilly's (search box at the bottom of the page) http://www.oreilly.com/reference/dictionary/tsearch.cgi
What Is? http://whatis.techtarget.com/
Cisco's Glossary of LAN terms http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb/glossary.htm
MobilInfo.Com Glossary http://www.mobileinfo.com/Glossary/
Free Online Dictionary Of Computing http://foldoc.doc.ic.ac.uk/foldoc/index.html
North Carolina ITS Glossary http://www.its.state.nc.us/Information/Glossary/GlossMain.asp
U. of Colorado Computing Standards with Links http://itp-www.colorado.edu/~scig/std_glossary.html

Appendix A: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines

The Department of Technology Planning is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as "Infrastructure Domains." The "Infrastructure Domains" and Governance are defined in the Commonwealth EA Glossary. The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. "IT Project Management" or "IT Project Oversight."

The following alpha codes will be used to identify each PSG:

Infrastructure Domains + Governance	**Code**
Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM ("Policy," "Standard," or "Guideline") XXXYYYY-ZZZ

    Where: XXX is the assigned Infrastructure Domain + Governance code;
                    YYYY is the year of initial issue; and
                    ZZZ is the sequential number assigned to link related PSG.

    Example: COV ITRM Standard GOV2000-01.1 is a standard that implements
                    COV ITRM Policy GOV2000-01.1.